UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/167,888	10/07/98	KAWELL, JR.	L 107755.117

EXAMINER	
KABAKOFF, S	
ART UNIT	**PAPER NUMBER**
2132	6

WM31/1002

JASON A REYES
HALE AND DORR
60 STATE STREET
BOSTON MA 02109

DATE MAILED: 10/02/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	Application No.	Applicant(s)	
	09/167,888	KAWELL, JR. ET AL.	
	Examiner	Art Unit	
	Steve Kabakoff	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 October 1998* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *5* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-39 have been examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. The term "substantially simultaneously" in **claims 22, 29, and 36** is a relative term which renders the claim indefinite. The term "substantially simultaneously" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

It is not clear whether two events occurring in a 1 minute interval is within the scope of "substantially simultaneously" as used in the claimed inventions, or whether the events would have to be within a specific time frame (milliseconds, microseconds, etc.) to meet the claim limitation.

4. The term "substantially prevent an unauthorized transfer" in **claim 31** is a relative term which renders the claim indefinite. The term "substantially prevent an unauthorized transfer" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. It is not clear what constitutes "substantial" prevention for transferring data.

5. **Claims 25, 32, and 39** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claimed inventions disclose a number (A-B) of end-user computers can get permission to access a data item from a publisher, a number (B-C) of end-user computers can get permission to access a data item from a distributor, and a number (C-1) of end-user computers can get permission to access a data item from a retailer.

However, the claims do not stipulate that B<A, C<B, and C>1 and therefore the claims would not make sense to one skilled in the art when any of these three equalities are not satisfied since it does not make sense to give a negative number of end-users permission to access a data item.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-6 and 8-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Comerford et al (US 5109413) in view of Stefik et al (US 5629980).

Claim 1: the claimed invention teaches transferring a single instance of permission to gain access to a data item from a first computer to a second computer and subsequently from the second computer to a third computer such that only the computer in possession of the permission can gain access to the data item.

Comerford et al (US 5109413) teaches a software asset protection mechanism that segregates software from a separate "right to execute" the software (see abstract). In Comerford et al (US 5109413), the right to execute is in the form of a decryption key called an application key AK (col. 1, lines 43-46) where the right to execute may be transferred from one user to another (col. 4, lines 40-50) such that the method of transferring a right to execute in Comerford et al (US 5109413) inherently allows the right to execute to be transferred from a first user's computer to a second user's computer then transferred again from the second user's computer to a third user's computer.

Since the right to execute is erased from a user's computer once it is transferred to a different user's computer (col. 7, lines 30-37 and col. 6, lines 5-9), only one user at a time can use a right to execute to access an encrypted application (col. 3, lines 25-30).

The method disclosed in Comerford et al (US 5109413) differs from the claimed invention since the right to execute in Comerford et al (US 5109413) permits a user to access *software*, whereas the permission in the claimed invention permits a user to access a *data item*.

Firstly, the examiner believes one of ordinary skill would understand the software taught in Comerford et al (US 5109413) is digital data, composed of binary information (ie, ones and zeros), and consequently falls within the scope of a general "data item."

Furthermore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the right to execute taught in Comerford et al (US 5109413) even in conjunction with non-executable digital data since it was well known in the art at the time of the inventions to distribute encrypted digital works, such as those in Stefik et al (US 5629980) (see abstract, col. 1, lines 60-67, and col. 9, lines 47-49), where the digital works would require a user to have a decryption key, such as the right to execute in Comerford et al (US 5109413), to gain access to the digital work.

One would be motivated to transfer non-executable digital works with a right to execute, as well as executable software, since electronic publishing companies at the time of the invention sold digital multimedia as well as software applications to make money (ie, col. 1, lines 10-24 in Stefik et al (US 5629980)).

Claims 2-3: the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980) described in regards to claim 1 uses a decryption key AK.

Claim 4: the right to execute permission in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980), decryption key AK, may be encrypted using a hardware vendor's key CSK (col. 5, lines 60-61 and col. 13, line 54 in Comerford et al (US 5109413)).

Claim 5: in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980), a hardware vendor key CSK may be used to encrypt a right to execute AK, where column 14, line 11 in Comerford et al (US 5109413) teaches the CSK may be a DES encryption key.

However, it was known in the art at the time of the inventions that public/private key pairs, such as industry standard RSA encryption keys used in SSL and PGP, were also available for cryptographic systems resistant to cryptanalytic attacks (see col. 27, lines 1-9 and col. 27, lines 20-23 in Stefik et al (US 5629980) or any basic cryptography text that was known in the art at the time of the invention, such as the Schneier reference cited at the end of this Office action).

Since the CSK in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980) is explicitly taught to be chosen for use in a cryptographic system resistant to plain text attacks (col. 14, lines 10-12 in Comerford et al (US 5109413)), clearly one of ordinary skill in the art would have found it obvious to choose the CSK as a public/private key as an

alternative to a symmetric DES key since both were known in the art of cryptography as being resistant to cryptographic attacks.

Claim 6: in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980), only the host computer (reference number 10 in Fig. 1 of Comerford et al (US 5109413)) having the right to execute AK stored in its memory (ie, see col. 1, lines 46-50 and reference number 20 in Fig. 1) can gain access to received encrypted data (E_{AK}(Application File) in Fig. 1).

Since the right to execute is erased from a user's computer once it is transferred to a different user's computer (col. 7, lines 30-37 and col. 6, lines 5-9 in Comerford et al (US 5109413)), only one user at a time can use a right to execute to access an encrypted application (col. 3, lines 25-30).

Claim 8: a user's computer (reference number 10 in Fig. 1 of Comerford et al (US 5109413)) in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980) inherently must comprise a de-encryptor that utilizes the right to execute, decryption key AK, so the user can gain access to a received digital work.

Claims 9-10: a host computer (reference number 10 in Fig. 1) having a secure link to a co-processor having temporary and permanent memory (col. 17, lines 35-44 and reference number 20 in Fig. 1 of Comerford et al (US 5109413)) in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980) stores the right to execute, decryption key AK, and uses AK to decrypt received digital works within the secure co-processor memory (col. 17, line 50 through col. 18, line 16 in Comerford et al (US 5109413)).

Claim 11: in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980), a transfer of a right to execute from one co-processor to another is considered safe when the two co-processors involved are able to identify one another as "members of the same

family" (col. 6, lines 23-32 in Comerford et al (US 5109413)). Therefore, a user's computer in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980) determines whether another user's computer is authorized to receive a right to execute before transferring that right to execute.

Claim 12: column 2, lines 23-38 in Comerford et al (US 5109413) disclose an expiration time rendering the transfer of a right to execute as temporary.

Claim 13: column 19, lines 23-30 in Comerford et al (US 5109413) disclose deleting a right to execute, decryption key AK, at an expiration time after the right to execute has been transferred to the permanent memory of a user's computer.

Claim 14: as previously discussed in regards to claim 1, in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980), the right to execute is erased from a user's computer once it is transferred to a different user's computer (col. 7, lines 30-37 and col. 6, lines 5-9), so only one user at a time can use a right to execute to access an encrypted application (col. 3, lines 25-30).

Claim 15: in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980), digital works are transferred from one user's computer to another, and a separate "right to execute" is transferred as well. In the abstract of Stefik et al (US 5629980), it is clear that one user computer would be an "owner" who transfers the digital work and the associated right to execute to a "buyer."

Thus, for a transaction between an "owner" and a "buyer" as taught in Stefik et al (US 5629980), it would have been obvious to one of ordinary skill in the art at the time of the invention to also include the transfer of funds in such an explicit commercial transaction as stated in column 3, lines 45-48 in Stefik et al (US 5629980).

Claim 16: column 23, lines 52-55 in Comerford et al (US 5109413) disclose a user's computer may have a "collection of rights to execute represented by the software decryption keys AK_1 and AK_2." Therefore, a user's computer must be able distinguish between more than one right to execute to gain access to a specific digital work in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980).

Claim 17: in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980), a first "owner" computer may operate in server mode before transferring a digital work to a second "buyer" computer (ie, col. 4, lines 10-12 in Stefik et al (US 5629980)). Stefik et al (US 5629980) discloses distributing digital works over the Internet (col. 1, lines 25-30), so it would have been obvious to one of ordinary skill in the art at the time of the invention to implement a computer running in "server mode" on the Internet as a Web server computer since the World Wide Web was known in the art to be a standard and ubiquitous means for communicating information over the Internet at the time of the invention.

Claims 18-19: column 1, lines 17-19 in Stefik et al (US 5629980) disclose the digital works in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980) include books, and column 4, lines 30-33 in Stefik et al (US 5629980) disclose including a rendering device for viewing a received digital work; thus, it is obvious that the rendering device would be a book viewing device when a user's computer in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980) receives a digital work comprising book data. Furthermore, it would be obvious that a functional rendering device for a digital work comprising book data would inherently comprise a viewing screen and appropriate communications circuitry.

Claims 20-24, 26-31, and 33-38: the claimed inventions comprise the same limitations as previously rejected claims 1-19 and are rejected for the same reasons. The examiner notes

that most of claims 20-24, 26-31, and 33-38 are broader in scope than previously rejected claims 1-19.

Claims 25, 32, and 39: the claimed inventions essentially teach having a publisher computer distribute permission data to a number A of end-user computers where the publisher computer delegates a number B of those permission datum to a distributor computer who in turn delegates a number C of those permission datum to a retailer computer who delegates one of the A permission datum to an end-user's computer.

The examiner believes such a publisher-distributor-retailer-enduser commercial hierarchy was well-known in business at the time of the inventions and it would have been obvious to one of ordinary skill in the art at the time of the invention to have a publisher computer in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980) having a collection of A rights to execute (ie, see col. 23, lines 52-55 in Comerford et al (US 5109413)) such that the A rights to execute $\{AK_1, AK_2, \ldots AK_A\}$ would be delegated according to an industry-standard business hierarchy comprising at least one distributor and retailer as well as a plurality of end-user consumers.

One of ordinary skill in the art would have been motivated to distribute the rights to execute in such an industry-standard hierarchy since it is common in business to have an end-user purchase digital works from any number of sources including directly from a publisher or distributor or retailer. Therefore, since buyers in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980) would seek digital works and their associated rights to execute from any number of different well-known commercial channels, each potential "owner" would have to possess a set of the requisite rights to execute (also see abstract in Stefik et al (US 5629980)).

8. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Comerford et al (US 5109413) in view of Stefik et al (US 5629980) as applied to claim 6 above, and further in view of Richards et al (US 6230267).

Claim 7: although the host computer, reference number 10 in Fig. 1 of Comerford et al (US 5109413), in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980) is not disclosed to be a "smartcard computer," the examiner believes it would be obvious to one of ordinary skill in the art at the time of the invention to implement the host in Comerford et al (US 5109413) on a portable smartcard such as the IC card in Richards et al (US 6230267).

In Figs. 1 and 2 in Richards et al (US 6230267), an IC card, which is known in the art to be a "smartcard" as recited in claim 7, receives application code and application data as part of an application unit (AU) and the IC card also receives a separate key transformation unit (KTU). The KTU comprises permission information relating to the encryption of the received AU which allows the IC card to decrypt the AU so the received application and data can be accessed by the IC card (col. 6, lines 53-60).

Clearly, the IC card in Richards et al (US 6230267) is analogous to the host computer in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980) since both receive digital data and separate permission data used to access the received digital data.

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the host computer in the combined method of Comerford et al (US 5109413) and Stefik et al (US 5629980) using a portable IC card, as taught in Richards et al (US 6230267), since a portable IC card gives a user flexibility of accessing various types of stored software and multimedia irrespective of different types of terminals where the user may choose to use the card (see col. 1, lines 28-34 in Richards et al (US 6230267)).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Schneier (Applied Cryptography, 2nd Ed.) – pages 47-52

Schmuck et al (US 6032216)

Berbec et al (US 6122631)

Foulston (US 5884308)

Komura et al (US 6260145)

Johnson et al (US 5175851)

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Steve Kabakoff whose telephone number is (703) 306-4153. The examiner can normally be reached on 8:30am to 6:00pm except every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert DeCady can be reached on (703) 305-9595. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

SK
SEK
September 20, 2001

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100